HMD Praxis der Wirtschaftsinformatik (2023) 60:283–307
https://doi.org/10.1365/s40702-023-00949-1

SCHWERPUNKT

Digitale Identitäten in der physischen Welt: Eine Abwägung von Privatsphäreschutz und Praktikabilität

Michael Roland · Tobias Höller · René Mayrhofer

Eingegangen: 18. September 2022 / Angenommen: 30. Januar 2023 / Online publiziert: 14. März 2023

Zusammenfassung Anforderungen an Datenschutz und Informationssicherheit, aber auch an Datenaktualität und Vereinfachung bewirken einen kontinuierlichen Trend hin zu plattformübergreifenden ID-Systemen für die digitale Welt. Das sind typischerweise föderierte Single-Sign-On-Lösungen großer internationaler Konzerne wie Apple, Facebook und Google. Dieser Beitrag beleuchtet die Frage, wie ein dezentrales, offenes, globales Ökosystem nach dem Vorbild des Single-Sign-On für die digitale, biometrische Identifikation in der physischen Welt aussehen könnte. Im Vordergrund steht dabei die implizite Interaktion mit vorhandener Sensorik, mit der Vision, dass Individuen in der Zukunft weder Plastikkarten noch mobile Ausweise am Smartphone mit sich führen müssen, sondern ihre Berechtigung für die Nutzung von Diensten rein anhand ihrer biometrischen Merkmale nachweisen können. Während diese Vision bereits jetzt problemlos durch Systeme mit einer zentralisierten Datenbank mit umfangreichen biometrischen Daten aller Bürger*innen möglich ist, wäre ein Ansatz mit selbstverwalteten, dezentralen digitalen Identitäten erstrebenswert, bei dem die Nutzer*in in den Mittelpunkt der Kontrolle über ihre eigene digitale Identität gestellt wird und die eigene digitale Identität an beliebigen Orten hosten kann. Anhand einer Analyse des Zielkonflikts zwischen umfangreichem Privatsphäreschutz und Praktikabilität, und eines Vergleichs der Abwägung dieser Ziele mit bestehenden Ansätzen für digitale Identitäten wird ein Konzept für ein dezentrales, offenes, globales Ökosystem zur privaten, digitalen Authentifizierung in der physischen Welt abgeleitet.

✉ Michael Roland · Tobias Höller · René Mayrhofer
Institut für Netzwerke und Sicherheit, Johannes Kepler Universität Linz, Linz, Österreich
E-Mail: michael.roland@ins.jku.at

Tobias Höller
E-Mail: tobias.hoeller@ins.jku.at

René Mayrhofer
E-Mail: rm@ins.jku.at

Schlüsselwörter eID · Privacy-by-Design · Biometrie · Authentifizierung · föderierte Identität · digitaler Zwilling

Digital Identities in the Physical World: A Trade-off Between Privacy and Practicability

Abstract Requirements on data privacy and information security, as well as data quality and simplification, cause a continuous trend towards federated identity systems for the digital world. These are often the single sign-on platforms offered by large international companies like Apple, Facebook and Google. This article evaluates how a decentralized, open, and global ecosystem for digital biometric identification in the physical world could be designed based on the model of federated single sign-on. The main idea behind such a concept is implicit interaction with existing sensors, in order to get rid of plastic cards and smartphone-based mobile IDs in a far future. Instead, individuals should be capable of proving their permissions to use a service solely based on their biometrics. While this vision is already proven feasible using centralized databases collecting biometrics of the whole population, an approach based on self-sovereign, decentralized digital identities would be favorable. In the ideal case, users of such a system would retain full control over their own digital identity and would be able to host their own digital identity wherever they prefer. Based on an analysis of the trade-off between privacy and practicability, and a comparison of this trade-off with observable design choices in existing digital ID approaches, we derive a concept for a decentralized, open, and global-scale ecosystem for private digital authentication in the physical world.

Keywords eID · Privacy-by-design · Biometrics · Authentication · Federated identity · Digital twin

1 Einleitung

Digitale Identitäten als Ausweise und Schlüssel für die virtuelle Welt haben einen festen Platz in unserem Leben eingenommen. Im eGovernment-Bereich ermöglicht es beispielsweise die digitale Signatur von Dokumenten (vgl. Richtlinie 1999/93/EG 2000 bzw. Signaturgesetz in Österreich, BGBl. I Nr. 190/1999), die Unterzeichnung von Verträgen und Formularen bei Behördenverfahren in die digitale Welt zu bringen (Austrian Federal Chancellery, Federal Platform Digital Austria 2014). Solche Signaturen können einfach zu Authentifizierungsmechanismen aufgewertet werden, um so das Ausweisen im Rahmen digitaler Behördenverfahren zu ermöglichen (vgl. Bürgerkarte und Handy-Signatur in Österreich (Austrian Federal Chancellery, Federal Platform Digital Austria 2014), nPA in Deutschland, e-ID in Estland, etc.) Harmonisierungsbestrebungen wie die eIDAS-Verordnung (Verordnung (EU) Nr. 910/2014) erweitern die Einsatzmöglichkeiten dieser Identitäten über die Landesgrenzen hinaus.

Für die Nutzung digitaler Identitäten in der physischen Welt gibt es zusätzlich die Herausforderung, dass eine digitale Identität konkret einer physisch anwesenden

Person zugeordnet werden muss. Aktuell wird dieses Problem oftmals durch das Ausgeben von Chipkarten gelöst, die mit einer digitalen Identität verknüpft werden. Personen werden also durch den Besitz (und eventuelle weitere Merkmale, wie eine PIN) der Chipkarte identifiziert. Hybride Identitätsdokumente, die sowohl analog als auch digital verifizierbar sein sollen, nutzen integrierte Chips um dafür biometrische Informationen über ihre Besitzer*in bereitzustellen (vgl. elektronische maschinenlesbare Reisedokumente nach ICAO Doc 9303 (2021) und Führerscheine nach ISO/IEC 18013-2:2020).

Das Aufkommen von Smartphones ermöglichte es, viele weitere Identitäten und Berechtigungsnachweise zu digitalisieren. So können wir z. B. Kundenkarten oder Tickets für Veranstaltungen und öffentliche Verkehrsmittel auf einem Gerät gesammelt bei uns tragen und über den Smartphone-Bildschirm bei einer Kontrolle jederzeit präsentieren. Eine breite Verfügbarkeit von NFC auf Smartphones führte dazu, dass auch wertvolle Identitäten für die physische Welt, wie zum Beispiel virtuelle Kreditkarten, Führerscheine (ISO/IEC 18013-5:2021) oder amtliche Lichtbildausweise (Bundesministerium für Finanzen 2022, ISO/IEC FDIS 23220-1 2022), zunehmend in Smartphones wandern. Das Smartphone wird dadurch zusehends zum Einstiegspunkt für eine Sammlung an digitalen Identitäten sowohl für die digitale, als auch für die physische Welt.

Science Fiction suggeriert seit geraumer Zeit, dass der nächste Schritt die Verdrängung des physischen Besitzfaktors zu Gunsten von biometrischer Identifikation sein könnte. Das Binden von digitalen Identitäten an biometrische Attribute würde das Mitführen von Ausweisdokumenten obsolet machen und Nutzern die Möglichkeit geben, durch explizite oder sogar implizite Interaktion mit biometrischen Sensoren, Aktionen in der physischen Welt auszulösen. Beispielsweise passen Werbetafeln im Film „Minority Report“ die Werbung im Vorbeigehen automatisch an die Identität der Betrachter*in an (Bonnette 2017).

Dass diese Vision bereits jetzt umsetzbar ist, zeigen Systeme wie Aadhaar in Indien (Unique Identification Authority of India 2022). Mit Aadhaar werden umfangreiche biometrische Referenzdaten aller Bürger*innen im Central Identities Data Repository, einer zentralisierten Datenbank, abgelegt. Öffentliche und private Dienste können biometrische Daten vom Central Identities Data Repository zur Authentifizierung von Personen und zum Zugriff auf deren staatliche eID verwenden (Unique Identification Authority of India 2022).

1.1 Implizite, digitale Authentifizierung in der physischen Welt

Ein möglicher Ansatz, um digitale Authentifizierung, nach dem Beispiel von Minority Report, auf die physische Welt und die implizite Interaktion mit Sensorik auszudehnen, ist die Modellierung der digitalen Identität als digitalen Zwilling[1] ihrer Inhaber*in. Dieser Zwilling umfasst sowohl die Modellierung von Bewegungsabläufe, Verhalten und Gewohnheiten des Individuums als auch die Anreicherung mit Attributen der digitalen Identität die Aktionen in der physischen Welt ermöglichen.

[1] Der digitale Zwilling ist ein Konzept aus dem Product-Life-Cycle-Management, das ursprünglich Grieves (mit einer Präsentation aus 2002) zugerechnet wird (Grieves und Vickers 2017; Barricelli et al. 2019).

Potential und Anforderungen eines globalen Ökosystems zur impliziten Nutzung einer digitalen Identität über die physische und digitale Welt hinweg lassen sich gut am Beispiel einer Flugreise mit Grenzübertritt veranschaulichen:

1. Zunächst bucht Anna im Onlineshop einer Fluglinie einen Flug von Washington, D.C. nach Wien. Sie meldet sich dazu mithilfe ihres digitalen Zwillings im Onlineshop an. Der Onlineshop bekommt damit Zugang zu ausgewählten Identitätsattributen und einer ihrer virtuellen Kreditkarten zur Bezahlung des Tickets. Nach erfolgter Zahlung wird das Ticket mit Annas digitaler Identität verknüpft.
2. Kurz vor dem Abflug checkt Anna für den Flug ein, wofür ein gültiges Reisedokument erforderlich ist. Annas digitaler Zwilling übermittelt die benötigten Attribute aus ihrem digitalen Reisepass und erhält im Gegenzug die Bordkarte als neuen Satz an Attributen.
3. Anna fährt mit dem Taxi zum Flughafen. Annas digitaler Zwilling erkennt das Ende der Fahrt und fragt am Display ihres Smartphones, ob sie die Fahrt mit einer ihrer Zahlungsmethoden bezahlen möchte. Anna bestätigt und der digitale Zwilling führt die Zahlung beim Taxiunternehmen durch.
4. Am Flughafen angekommen, möchte Anna ihr Gepäck aufgeben. Die Videokamera des Check-In-Automaten detektiert Annas Gesicht und bestätigt ihrem digitalen Zwilling, dass sich Anna vor dem Automaten befindet. Der digitale Zwilling übermittelt daraufhin die notwendigen Flug- und Passagierdaten aus der Bordkarte um das Gepäckstück der Passagierin zuzuordnen und die Einhaltung der Freigepäckmenge sicherzustellen. Nach Abgabe des Koffers erhält Anna eine Bestätigung über die Gepäckaufgabe in ihren digitale Zwilling.
5. Anschließend begibt sich Anna zur Sicherheitskontrolle um in den Transitbereich zu gelangen. Sobald die Videokamera an der Schleuse Annas Gesicht erkennt, kann ihr digitaler Zwilling die notwendigen Informationen übermitteln, um die Schleuse zu öffnen.
6. Nach einiger Wartezeit hat es Anna endlich in den Transitbereich geschafft. Sie betritt einen Duty-Free-Shop, um eine Flasche Wasser und eine edle Flasche Whiskey zu kaufen. An der Kasse angelangt, bezahlt Anna mittels Fingerabdruck. Mit dem Fingerabdruck kann der Shop Annas digitalen Zwilling davon überzeugen, dass Anna bezahlen möchte. Die Kassa benötigt dafür, neben der Zahlungsinformation, die Bestätigung, dass Anna zumindest 21 Jahre alt ist und eine Bordkarte für einen Auslandsflug besitzt.
7. Da ihr Flug Verspätung hat beschließt Anna, sich vor dem Abflug noch ein wenig in der Business-Class-Lounge der Fluglinie zu entspannen. Die Videokameras am Weg zur Lounge detektieren Annas Gesicht und informieren ihren digitalen Zwilling darüber, dass Anna sich auf dem Weg zur Lounge befindet. Der digitale Zwilling öffnet daher die Tür zur Lounge, sobald Anna davor angekommen ist, indem er den Nachweis übermittelt, dass Anna eine gültige Business-Class-Bordkarte (oder den Frequent-Traveller-Status) besitzt.
8. Der Abflug steht kurz bevor, das Boarding hat begonnen. Die Kamera am Gate detektiert Annas Gesicht, woraufhin ihr digitaler Zwilling bestätigt, dass Anna eine gültige Bordkarte für diesen Flug besitzt. Daraufhin darf Anna das Flugzeug betreten.

9. Endlich im Flugzeug und am Sitzplatz angekommen, ist Anna genervt: Es sitzt schon jemand auf ihrem Platz. Anna nimmt ihr Smartphone und überprüft die in ihrer digitalen Identität gespeicherte Bordkarte. Der Sitzplatz stimmt. Mit der Sitzplatzinformation am Smartphone-Display klärt Anna die andere Person über ihren Fehler auf.
10. Nach einem langen Flug ist Anna in Wien angekommen und steht an der Passkontrolle. Anna blickt dazu in eine Videokamera und hält ihren Zeigefinger auf einen Fingerabdrucksensor. Daraufhin übermittelt der digitale Zwilling den digitalen Reisepass an den Grenzposten. Der Grenzposten überprüft die Daten, stellt fest, dass Anna die notwendigen Voraussetzungen für den Grenzübertritt erfüllt, und lässt sie passieren.

Obwohl dieses Beispiel viele, sehr unterschiedliche Anwendungsszenarien für digitale Identitäten beinhaltet, lassen sich in Bezug auf die benötigten Komponenten eindeutige Gemeinsamkeiten ableiten. Jede Nutzung einer digitalen Identität in der physischen Welt entsteht durch das Zusammenspiel von vier Komponenten, das in Abb. 1 dargestellt wird (vgl. Mayrhofer et al. 2020):

1. *Individuum:* Das Individuum ist eine natürliche Person, die in der physischen Welt agiert. Als Nutzer*in des ID-Ökosystems ist das Individuum Inhaber*in einer (oder sogar mehrerer) digitaler Identitäten.
2. *Sensor:* Sensoren bilden Aktionen des Individuums in der physischen Welt auf Ereignisse in der digitalen Welt ab.
3. *Identity Agent:* Als digitaler Zwilling repräsentiert der Identity Agent (vgl. „Identity in the Cloud Agent“, Ates et al. 2011) das Individuum in der digitalen Welt

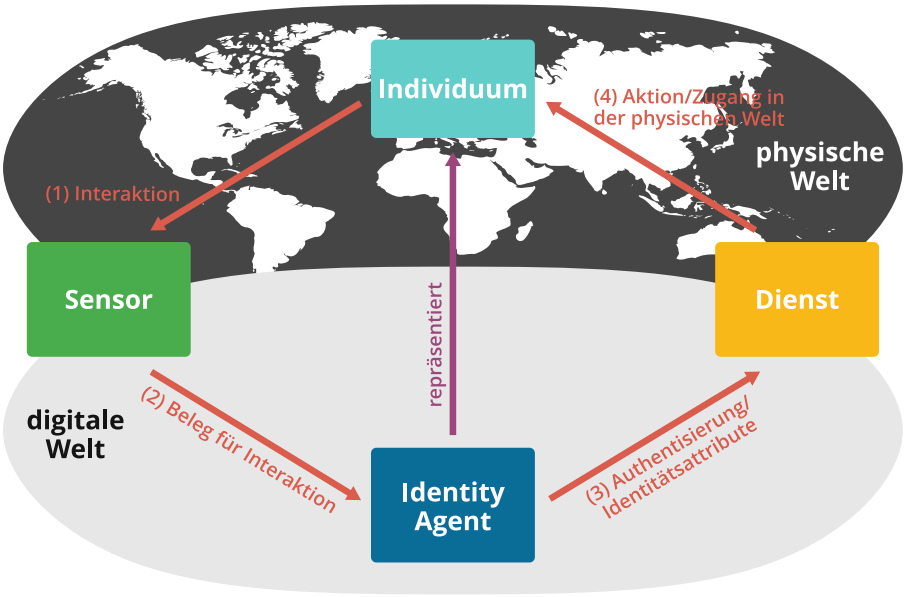

Abb. 1 Interaktion zwischen den Komponenten beider Welten

und verwaltet als ID-Wallet eine Sammlung an digitalen Identitäten einer Person. Anhand von, durch Sensoren gelieferten, Ereignissen werden Bewegungsabläufe, Verhalten und Gewohnheiten des Individuums modelliert und mit Attributen der digitalen Identitäten verknüpft, um daraus auf aktuelle Intentionen des Individuums zu schließen und Vorhersagen über zukünftige Handlungen zu treffen. Auf Basis erkannter Intentionen löst der Identity Agent Authentisierungen bei zuständigen Diensten aus und übermittelt die notwendigen Identitätsattribute, welche die Berechtigung zur Nutzung des Dienstes belegen.

4. *Dienst:* Der Dienst stellt berechtigten Individuen seine Leistungen bereit. Er bildet also Aktionen des Identity Agents aus der digitalen Welt auf Reaktionen für das Individuum in der physischen Welt ab, sofern das Individuum dazu autorisiert ist.

Systeme wie Aadhaar (Unique Identification Authority of India 2022) zeigen, dass derartige Systeme mit aktueller Technologie bereits umgesetzt werden können, wenn es eine zentrale Stelle zur biometrischen Authentifizierung gibt. Allerdings hat sich auch gezeigt, dass die Konzentration von digitalen Identitäten zu technischen und gesellschaftlichen Problemen führen kann. Im Fall von Aadhaar hat sich gezeigt, dass Schwachstellen in der Absicherung solcher Datenbanken katastrophale Folgen haben können (Khaira 2018). Gleichzeitig zeigt die weitreichende biometrische Überwachung in China (Qian et al. 2022), welches Potential zur totalen Überwachung solche Datenbanken auf Basis biometrischer Informationen bieten können.

1.2 Zielsetzung und Methodik

Die implizite Interaktion mit biometrischen Sensoren im öffentlichen Raum stößt, zumindest in der Europäischen Union, auf breite Ablehnung (Schaber et al. 2020). Die rechtlichen Rahmenbedingungen würden derzeit ein solches System nicht zulassen (vgl. EU-Datenschutz-Grundverordnung, Verordnung (EU) 679/2016), sofern die Privatsphäre unbeteiligter damit verletzt werden könnte[2]. Während diese invasiven Systeme im Idealfall auf regulativer Ebene verhindert und eingeschränkt werden, könnte der Wunsch der Gesellschaft, sich die Vorteile dieser Technologie nutzbar zu machen, hier mittelfristig zu einer Änderung der Rechtslage führen. Diese Arbeit geht davon aus, dass implizite biometrische Identifikation im öffentlichen Raum in Zukunft umgesetzt werden könnte, und analysiert, wie den davon ausgehenden Risiken auf technischer Ebene entgegen gesteuert werden kann. Die Betrachtung in dieser Arbeit fokussiert sich auf Privacy-by-Design daher vorwiegend im Sinne von Privacy-by-Architecture auf technischer Ebene und weitgehend losgelöst von einer Betrachtung im Sinne von Privacy-by-Policy auf regulativer Ebene (vgl. Danezis et al. 2014; Phillips 2004).

Um den Risiken einer zentralen Datenbank entgegenzusteuern, ist ein dezentraler, benutzerzentrischer Ansatz für die biometrische Identifikation erstrebenswert. Dieser

[2] Dass der Betrieb eines solchen Systems auch im öffentlichen Raum, unter Einhaltung entsprechender Maßnahmen zum Schutz von Persönlichkeitsrechten, aus Sicht der österreichischen Datenschutzbehörde zulässig sein kann, zeigt deren Genehmigung eines Feldversuchs an der Johannes Kepler Universität Linz, vgl. https://www.digidow.eu/jku-face-recognition.

Artikel erarbeitet ein Konzept für ein solches offenes, globales, dezentrales Ökosystem zur impliziten, digitalen Identifikation in der physischen Welt. Die Nutzer*in soll dabei in den Mittelpunkt der Kontrolle über ihre eigene digitale Identität und die eigenen Daten gestellt werden. Anhand einer schrittweisen Auftrennung von Rollen, Verantwortung und Infrastruktur wird analysiert, wie dadurch die Privatsphäre der Nutzer*innen gestärkt werden kann und welche neuen Probleme (insbesondere in Hinblick auf Komplexität) durch diese Dezentralisierung verursacht werden, die ein solches System impraktikabel machen würden. Wir analysieren diesen Zielkonflikt zwischen umfangreichem Privatsphäreschutz und Praktikabilität, und vergleichen die Abwägung dieser Ziele mit anderen, insbesondere europäischen Ansätzen für digitale Identitäten. Schlussendlich leiten wir daraus ein Konzept ab, um eine zentrale (biometrische) Identitätsdatenbank in dezentrale, persönliche Identity Agents zu überführen.

2 Rollen und Datenflüsse

Die grundlegenden Komponenten eines ID-Ökosystems zur impliziten digitalen Authentifizierung in der physischen Welt lassen sich, anhand des Beispiels aus Abschn. 1.1, weiter in spezifische Rollen gliedern:

1. *Individuum:* Anna wird durch ihre Sammlung an digitalen Identitäten in der digitalen und der physischen Welt repräsentiert. Sie möchte, dass Dienste bestehende Identitätsattribute verwenden (z. B. Altersnachweis, Zutrittsberechtigung) und neue Attribute mit ihrer Identität verknüpfen können (z. B. Bordkarte). Anna möchte explizit *nicht*, dass Dienste Zugriff auf andere als die benötigten Attribute erlangen oder Interaktionen ohne ihre Zustimmung miteinander verknüpfen. Darüber hinaus möchte Sie mit ihrer digitalen Identität explizit interagieren können (z. B. Freigabe eine Bezahltransaktion, Login bei Online-Service, Anzeige der Sammlung an Identitätsattributen, Freigabe von Attributen an einen Dienst).
2. *Verhaltensmodell (Identity Agent):* Das Verhaltensmodell ist Annas digitaler Zwilling. Dieser modelliert, auf Basis von Messdaten und der Sammlung von Identitätsattributen, Annas Bewegungsabläufe, Verhalten und Gewohnheiten, und leitet so Aussagen bzw. Vorhersagen über ihre Handlungen ab. Der Identity Agent stößt damit selbstständig Interaktionen bei Diensten an (z. B. Zahlung im Taxi, Kofferaufgabe, Zutritt) und nimmt neue Identitätsattribute auf (z. B. Gepäckschein, Zahlungsbestätigung).
3. *ID-Wallet:* Die ID-Wallet ist der Datenspeicher für Annas digitale Identitäten. Identitätsattribute können darin abgelegt werden (z. B. Name, Geburtsdatum, biometrische Merkmale, Bordkarte, Gepäckschein) und bei Bedarf an Dienste zur Authentifizierung übermittelt werden (z. B. Zutrittsberechtigung, Altersnachweis). Darüber hinaus gibt die ID-Wallet Anna die Möglichkeit, sich einen Überblick über ihre eigene digitale Identität zu verschaffen (z. B. Sitzplatzinformation auf der Bordkarte).
4. *Sensoren:* Sensoren bilden die Brücke von der physischen Welt in die digitale Welt. Sie nehmen Annas Interaktionen mit der physischen Welt auf und geben

diese Informationen an den Identity Agent weiter. Sensoren können dabei auf explizite Interaktionen (z. B. Auflegen des Fingers auf einen Fingerabdrucksensor, Drücken eines Tasters, Vorhandensein eines physischen Tokens) oder auf implizite Interaktionen (z. B. Vorbeigehen an einer Videokamera, Messung von Position oder Bewegungsart) ausgelegt sein. Sie können fest an eine bestimmte Reaktion in der physischen Welt (z. B. Kamera/Fingerabdrucksensor an einer einzelnen Schleuse) oder fest an ein bestimmtes Individuum (z. B. Positions- und Aktivitätsmessung im mitgeführten Smartphone) gekoppelt sein, oder auch losgelöst von einzelnen Diensten und Individuen, in der gesamten Infrastruktur verteilt sein (z. B. Überwachungskameras im öffentlichen Raum am Weg zur Lounge).

5. *Aktoren:* Analog zu den Sensoren bilden Aktoren die Brücke von der digitalen Welt zurück in die physische Welt. Sie setzen autorisierte Reaktionen auf Annas Interaktionen um. Das können automatisierte Aktionen (z. B. das Öffnen einer Tür oder Schleuse) aber ebenso manuelle Handlungen (z. B. das Aushändigen von Waren durch Kassier*in) sein.
6. *Verifier:* Der Verifier (vgl. Camenisch et al. 2014) ist die authentifizierende Stelle für einen von Anna genutzten Dienst. Er verifiziert, dass Sensormessungen und Attribute authentisch sind.
7. *Referenzmonitor des Dienstes:* Den Übergabepunkt zwischen Verifier und Aktor bildet der Referenzmonitor des Dienstes. Dieser prüft, anhand der durch den Verifier authentisierten Informationen, ob Anna zu einer bestimmten Aktion bei diesem Dienst autorisiert ist (z. B. Inhaberin einer Bordkarte, des Frequent-Traveller-Status, bestätigte Bezahlung) und steuert den Aktor an.
8. *Herausgeber:* Herausgeber (oft auch als Identity Provider (IdP), Issuing Authority (IA) oder Issuer bezeichnet) sind Stellen, die Attribute zu Annas Identitäten beisteuern. Sie können Attribute ausstellen (und ggf. auch zurückziehen), die Anna in ihre ID-Wallet mit aufnehmen kann. Eine solche Stelle könnte z. B. der Staat sein, der Anna eine Basisidentität bestehend aus ihrem Namen, Geburtsdatum, verifizierten biometrischen Merkmalen, etc. bereitstellt. Ebenso können Dienste Identitätsattribute ausstellen. Diese können an den einzelnen Dienst gebunden sein (virtuelle Bezahlkarte zur Freigabe von Transaktionen bei einer Bank, Gepäckschein als Beleg der Gepäckaufgabe bei einer Fluglinie) oder über mehrere Dienste hinweg genutzt werden (z. B. Zahlungsbeleg einer Bank, Bordkarte).

Bei der Betrachtung der Dezentralisierung der Komponenten im ID-Ökosystem sind die Datenflüsse und daraus entstehende Vertrauensbeziehungen zwischen diesen Rollen von entscheidender Bedeutung. Diese geben Aufschluss, welche Vor- oder Nachteile sich aus der Trennung von Rollen für die Privatsphäre des Individuums sowie für die Skalierbarkeit, Komplexität und Realisierbarkeit dieser Schnittstellen ergeben können. Anhand des Beispiels aus Abschn. 1.1 lassen sich folgende Datenflüsse und Vertrauensbeziehungen (siehe Tab. 1) bestimmen:

- *Individuum und Identity Agent:* Das Individuum wird durch den Identity Agent (Verhaltensmodell) repräsentiert. Der Identity Agent fordert somit ultimatives Vertrauen des Individuums über eine akkurate Repräsentation (Anna möchte mög-

lichst exakt modelliert werden). Der Datenfluss erfolgt ausschließlich indirekt über Sensoren und die ID-Wallet.

- *Individuum und ID-Wallet:* Die ID-Wallet ermöglicht dem Individuum eine Verwaltung ihrer digitalen Identität. Die ID-Wallet informiert das Individuum über gespeicherte Attribute (z. B. Sitzplatzinformation der Bordkarte) und über Transaktionen (z. B. Bezahltransaktion). Bei Bedarf kann auch ein explizites Einverständnis für Interaktionen vom Individuum eingeholt werden (z. B. Freigabe einer Bezahltransaktion, Login bei Online-Diensten).
- *Individuum und Sensoren:* Die Sensoren erheben biometrische Merkmale und Interaktionsdaten von Individuen. Bei impliziter Interaktion werden dabei u.U. auch Daten von außenstehenden Individuen, die nicht Teil des ID-Ökosystems sind, ohne deren explizites Einverständnis erhoben (z. B. Überwachungskamera im öffentlichen Raum).
- *Individuum und Aktoren:* Aktoren bewirken Reaktionen der physischen Welt für Individuen.
- *Individuum und Herausgeber:* Herausgeber attestieren einem Individuum neue Attribute. Der Datenfluss zwischen Individuum und Herausgeber erfolgt jedoch indirekt über die ID-Wallet (zur Verknüpfung und Speicherung von Attributen) und ggf. über Sensoren (zur initialen Messung biometrischer Merkmale). Letztere werden jedoch aufgrund ihrer engen Bindung an den Herausgeber und die ausschließliche Verwendung zur initialen Aufnahme neuer biometrischer Merkmale in dieser Betrachtung außer Acht gelassen.
- *ID-Wallet und Herausgeber:* Herausgeber liefern neue oder geänderte Attribute in die ID-Wallet des Individuums ein und können diese ggf. auch wieder zurückziehen. Neben einer (oder sogar mehreren, unabhängigen) Basisidentitäten, soll die ID-Wallet zusätzliche Attribute von beliebigen Herausgebern aufnehmen können. Vergleichbare Anforderungen finden sich bereits in bestehenden eID-Wallet-Konzepten (vgl. europäische digitale Identität (Europäische Kommission 2021) und SSI-Projekte wie z. B. Sovrin, Windley 2021).
- *Identity Agent und Herausgeber:* Der Identity Agent muss, bei Nutzung von (insb. biometrischen) Attributen aus der ID-Wallet, auf die korrekte Zuordnung von Attributen zum Individuum durch den Herausgeber vertrauen.
- *Identity Agent und ID-Wallet:* Der Identity Agent benötigt zur möglichst genauen Modellierung des digitalen Zwillings einen Überblick über alle Attribute der digitalen Identitäten eines Individuums und deren potentielle Einsatzmöglichkeiten (also die für das Individuum relevanten Dienste). Der Identity Agent stößt auch die Herausgabe von Attributen aus der ID-Wallet an Verifier an. Während im Sinne einer potentiellen Entkopplung die Rolle des Verhaltensmodells und des Datenspeichers für die digitale Identität von einander getrennt wurden, benötigen diese uneingeschränkten Datenaustausch und gegenseitiges Vertrauen. Die Betrachtung von Identity Agent und ID-Wallet als eine untrennbare Einheit erscheint daher zweckmäßig.
- *Identity Agent und Sensoren:* Sensoren liefern Messergebnisse von Ereignissen aus der physischen Welt an den Identity Agent. Der Identity Agent muss dazu den Sensoren vertrauen, dass diese authentische Messergebnisse liefern.

Tab. 1 Datenflüsse und Vertrauensbeziehungen (D: Datenfluss von Attributen (Personenbezug), (D): sonstiger Datenfluss; V: Vertrauen, (V): schwaches Vertrauen, –: kein Datenfluss/Vertrauensbeziehung, •: nicht anwendbar [Selbstbezug])

von \ zu	Individuum	Identity Agent	ID-Wallet	Sensoren	Aktoren	Verifier	Referenzmonitor	Herausgeber
Individuum	•	V	(D)/V	D	–	–	–	–
Identity Agent	–	•	D/V	V	–	D/(V)	–	–
ID-Wallet	D	D/V	•	–	–	D/(V)	–	–
Sensoren	–	D	–	•	–	–	–	–
Aktoren	(D)	–	–	–	•	–	V	–
Verifier	–	(V)	–	V	–	•	D/V	V
Referenzmonitor	–	–	–	–	(D)	V	•	–
Herausgeber	–	V	D	–	–	D	–	•

- *Identity Agent und Verifier:* Der Identity Agent aktiviert den Verifier und übergibt diesem Attribute zur Authentifizierung einer Interaktion. Der Verifier muss dabei ggf. auf Aussagen über Handlungsabläufe (z. B. Anna bewegt sich auf Tür zu) des Identity Agents vertrauen, wobei diese durch entsprechende Sensorbelege gestützt sein können. Der Identity Agent muss, umgekehrt, dem Verifier vertrauen, dass dieser sorgsam mit den übertragenen Daten umgeht.
- *Verifier und Sensoren:* Neben den vom Identity Agent abgeleiteten Aussagen über Intentionen des Individuums, werden diese auf Messergebnisse von Sensoren gestützt. Der Verifier muss daher bei der Verifikation dieser Aussagen auf eine akkurate Messung durch die Sensoren, untermauert durch entsprechende Belege, vertrauen.
- *Verifier und Herausgeber:* Zur Authentifizierung von Attributen muss der Verifier den Herausgebern dieser Attribute vertrauen und ggf. über den Rückruf von Attributen informiert werden (vgl. Hölzl et al. 2018 zu Maßnahmen gegen damit einhergehende Datenleaks).
- *Verifier und Referenzmonitor:* Der Verifier authentisiert Attribute und gibt die für eine Autorisierung von Aktionen relevanten Informationen an den Referenzmonitor weiter (z. B. Zutritts- bzw. Zugriffsberechtigung, bezahlte Leistung, Altersnachweis). Der Referenzmonitor muss dazu der Verifikation und akkuraten Datenweitergabe durch den Verifier uneingeschränkt vertrauen. Ebenso muss der Verifier darauf vertrauen, dass der Referenzmonitor die Daten ausschließlich zur Berechtigungsprüfung verwendet.
- *Referenzmonitor und Aktoren:* Der Referenzmonitor prüft die Autorisierung von Handlungen des Individuums anhand der zur Verfügung stehenden Attribute und veranlasst entsprechende Aktionen durch die Aktoren. Der Aktor muss dabei dem Referenzmonitor uneingeschränkt vertrauen.

Für die Verbesserung des Privatsphäreschutzes durch Dezentralisierung werden insbesondere jene Schnittstellen relevant sein, über die personenbezogene oder sensible Daten übermittelt werden (vgl. Datenflüsse in Tab. 1). Dabei erscheinen vor

allem der Übergabepunkt zwischen ID-System und Diensten (Verifier, Referenzmonitor und Herausgeber), die Sensoren, und der Identity Agent samt zugehörigem Datenspeicher (ID-Wallet) als Punkte für mögliche Entkopplungen und Dezentralisierungsstrategien in Frage zu kommen.

3 Privatsphäre durch Dezentralisierung

Basierend auf der Analyse der unterschiedlichen Rollen in einem digitalen Identitätssystem kann man nun die Frage stellen, ob diese sinnvoll durch dezentralisierte Systeme erfüllt werden können. Der Begriff der Dezentralisierung umfasst dabei zwei unterschiedliche Aspekte:

1. *Organisatorisch:* Die Rollen sollen von organisatorisch getrennten Entitäten unabhängig wahrgenommen werden können.
2. *Räumlich:* Die Hardware, auf der die für eine Rolle notwendigen Schritte ausgeführt werden, soll räumlich verteilt sein können.

Besonderer Fokus wird auf die Identifikation neuer Herausforderungen gelegt, die sich durch die dezentrale Erfüllung von Rollen ergeben.

3.1 Dezentralisierung der Dienste

Die Dezentralisierung der Dienste stellt auf den ersten Blick die geringste Herausforderung dar, da auch bereits etablierte Systeme wie Aadhaar das Ziel haben, die Authentisierung für externe Dienste zu übernehmen. Die Idee von räumlich unabhängigen Diensten ist an dieser Stelle also kein Novum. Schwieriger wird es schon bei der organisatorischen Unabhängigkeit. Diese beginnt bei Aadhaar an der Schnittstelle zwischen Verifier und Referenzmonitor (vgl. auch Schlager et al. 2006): Aadhaar stellt die Authentisierung und der Dienst prüft lediglich die Autorisierung bei uneingeschränktem Vertrauen in die zentrale Datenbank. Das zentrale System schränkt die organisatorische Unabhängigkeit der Dienste sogar noch weiter ein, indem Dienste eine offizielle Erlaubnis brauchen, bevor sie das digitale Identitätssystem nutzen können. Aadhaar ist hier jedoch kein Einzelfall; auch Berechtigungszertifikate für den Zugriff auf den nPA in Deutschland folgen einem ähnlichen Prinzip, wenngleich hierbei der Dienst den Verifier mit einschließt. Die Erlaubnis von offizieller Stelle hat den großen Vorteil, dass Benutzer*innen mehr Vertrauen zu den Anbietern von Diensten haben können, widerspricht aber gleichzeitig dem Ziel der organisatorischen Unabhängigkeit. Ein offenes System hat jedoch den Nachteil, dass Nutzer*innen davon ausgehen müssen, dass manche Dienste versuchen werden, das System zu missbrauchen, um Daten von Individuen zu stehlen.

Damit wird die Frage, welche Attribute man welchen Diensten zugänglich machen sollte, besonders relevant. Nach Zwingelberg und Hansen (2011) lassen sich drei Arten von Transaktionen unterscheiden, die unterschiedliche Attribute mit einem Dienst teilen:

- Identifikation, also die Weitergabe von Attributen, die eine eindeutige, globale Unterscheidung der digitalen Identität ermöglichen;
- pseudonyme Authentifizierung, also die Weitergabe von Attributen, die lediglich in einem abgrenzbaren Bereich, z. B. bei einem einzelnen Diensteanbieter, eine eindeutige Zuordnung der digitalen Identität zu vorhergehenden und nachfolgenden Transaktionen ermöglichen (vgl. Ableitung dienstespezifischer Pseudonyme nach Jøsang und Pope (2005), Attribute Management Principles nach Chivers (2005), Authentifizierung mit FIDO UAF/U2F[3]); und
- anonyme Authentifizierung, also die Weitergabe von Attributen, die lediglich eine Mitgliedschaft in einer Gruppe, z. B. den Besitz eines gültigen Tickets, bestätigen.

In vielen Fällen kann eine anonyme Authentifizierung völlig ausreichend sein. So z. B. bei der Verifikation der Bordkarte im Duty-Free-Shop: Dort ist nur der Besitz einer Bordkarte für einen Auslandsflug relevant. Es muss nicht zwischen mehreren Nutzungen derselben Bordkarte unterschieden werden. Auch der Name auf der Bordkarte oder das konkrete Flugziel sind belanglos für den Shop (wenngleich dies mitunter dem Interesse des Diensteanbieters zur Analyse von Kundenbeziehungen – über das erforderliche Mindestmaß hinaus – entgegenstehen könnte).

Viele andere Szenarien wie zum Beispiel die Gepäckaufgabe oder der Nachweis eines gültigen digitalen Reisepasses können durch eine pseudonyme Authentifizierung erfolgen. Dabei werden sowohl dem Passagier als auch dem digitalen Reisepass ein zufälliger Code zugewiesen, den nur der Herausgeber des Attributs auflösen kann. So kann die Fluglinie das Gepäck den einzelnen Passagieren zuordnen, ohne bei der Gepäckaufgabe nach einem identifizierenden Merkmal zu fragen. Die Fluglinie kann sogar überprüfen, ob der digitale Reisepass gültig ist, ohne dessen Inhalt zu kennen, indem es einfach bei der Behörde nachfragt. Durch diesen Verzicht auf die Weitergabe von identifizierenden Attributen kann das Risiko durch missbräuchliche Dienste für die meisten Szenarien auf ein akzeptables Maß reduziert werden. In bestimmten Situationen, besonders wenn der Abgleich mit anderen Datenquellen erforderlich ist, ist die Übermittlung von identifizierenden Attribute jedoch unvermeidlich. Bei der Grenzkontrolle könnte beispielsweise ein Abgleich mit, abseits des ID-Ökosystems gepflegten, Sperrlisten auf denen nur Name und Geburtsdatum eingetragen sind, notwendig sein.

Konzepte aus dem Bereich der Attribute-Based-Credentials (ABC) und der Self-Sovereign-Identity (SSI) sorgen dafür, dass immer mehr Szenarien mit pseudonymer und anonymer Identifikation umgesetzt werden können. ABC (Koning et al. 2014) ermöglichen die selektive Weitergabe von Attributen oder auch Aussagen über Attribute (z. B. die Behauptung, eine gewisse Altersschwelle erreicht zu haben, statt das vollständige Geburtsdatum preiszugeben). Verifiable Presentations (Sporny et al. 2022a) und Decentralized Identifiers (Sporny et al. 2022b) aus dem Bereich der SSI ermöglichen das Zusammenstellen von Credentials zu einer Aussage (z. B. einem Credential der Identitätsdatenbank über die Erkennung des Individuums an einem bestimmten Ort und einem Credential über den Besitz einer gültigen Bordkarte).

[3] https://fidoalliance.org/how-fido-works/.

Diese Methoden sind aktuell dabei, sich in den verschiedensten Identitätsanwendungen zu etablieren. So ist die selektive Weitergabe von Attributen fester Bestandteil verschiedener ISO-Normen zu mobilen digitalen Identitäten (ISO/IEC 18013-5:2021; ISO/IEC FDIS 23220-1 2022), wird in SSI-Projekten forciert (Sovrin[4], Evernym[5], Jolocom[6], IDunion[7], etc.) und ist auch in verschiedenen nationalen ID-Schemata in der EU (z. B. seit geraumer Zeit im nPA in Deutschland (Poller et al. 2012) und seit kurzem in der ID-Austria (A-SIT Plus GmbH 2021a)) umgesetzt. Wir gehen daher davon aus, dass ein dezentrales System zur digitalen Authentifizierung in der physischen Welt nur in Ausnahmefällen identifizierende Attribute weitergeben würde, weil die meisten Anwendungsszenarien durch die Zusammenstellung mehrerer ABCs abgebildet werden können.

3.2 Dezentralisierung der Sensoren

Analog zu Diensten sind auch Sensoren in zentralisierten Systemen bereits verteilt, weswegen nur die organisatorische Dezentralisierung genauer betrachtet werden muss. Da Sensoren biometrische Daten erfassen, ist es aus Sicht der Datensparsamkeit zu bevorzugen, wenn mehrere kleinere Organisationen Sensoren betreiben, weil so die Menge der Daten, die einzelnen Organisationen zur Verfügung stehen, reduziert wird. Wenn allerdings jeder seine eigenen Sensoren betreiben darf, stellt sich erneut die Frage des Vertrauens in die Betreiber von Sensoren. Identity Agents müssen Sensoren vertrauen können, da sie ihre Entscheidung, Attribute an Dienste zu übermitteln, auf die Messergebnisse von Sensoren stützen. Dienste sind ebenfalls auf die Sensoren angewiesen, um digitale Attribute einzelnen Individuen zuzuordnen.

Bevor dieses Problem weiter analysiert werden kann, muss eine weitere Frage gestellt werden: Wo erfolgt der Abgleich der vom Sensor gemessenen Daten mit den gespeicherten biometrischen Templates der Individuen? Wenn dieser am Sensor erfolgen soll, dann benötigt jeder Sensor Zugriff auf die biometrischen Templates von potentiellen Nutzern, wodurch noch mehr Vertrauen in Sensoren erforderlich wird. Alternativ könnten die gemessenen Daten auch direkt an den Identity Agent übermittelt werden, welcher daraufhin den Abgleich der biometrischen Informationen vornimmt. Dieser Ansatz ist für Systeme mit einem zentralen Identity Agent (wie Aadhaar) gut geeignet, führt jedoch zu Problemen bei vielen verteilten Identity Agents. Die verteilten Identity Agents würden in diesem Fall alle Zugriff auf die Sensordaten (und damit die biometrischen Templates aller Individuen; selbst jener, die nicht am ID-System teilnehmen) bekommen. Effektiv müsste daher jedes Individuum allen Identity Agents vertrauen können, was in der Praxis kaum umsetzbar sein dürfte.

Aus dieser Überlegung heraus erscheint der Abgleich von biometrischen Templates auf den Sensoren als sinnvollster Ansatz. Dies würde gleichzeitig auch die Privatsphäre unbeteiligter Individuen stärken, indem Sensoren biometrische Daten

[4] https://sovrin.org/.

[5] https://www.evernym.com/.

[6] https://jolocom.io/.

[7] https://idunion.org/.

von nicht erkannten Individuen unmittelbar verwerfen können und diese damit keiner weiteren Verarbeitung oder Übermittlung unterliegen. Allerdings wäre eine Übertragung aller vorhandenen Templates in einem globalen System sowohl in Hinblick auf die Privatsphäre, als auch in Hinblick auf die Performance (bzw. die Leistungsanforderungen an den Sensor) unverhältnismäßig. Praktikabel wird dieses Szenario erst, wenn der Sensor nur einen Teil der biometrischen Templates bekommt; nämlich jene, die für eine Interaktion auch in Frage kommen.

Sensoren müssen also genug Vertrauen bei Identity Agents aufbauen, damit diese ihnen deren biometrische Templates für Vergleiche zur Verfügung stellen, und gleichzeitig das uneingeschränkte Vertrauen der Dienste besitzen, die sich auf ihre Aussagen verlassen. Es kann daher davon ausgegangen werden, dass viele Dienste ihre eigenen Sensoren betreiben möchten, um das Vertrauensproblem zwischen Verifier und Sensor zu eliminieren. Der Fingerabdrucksensor im Duty-Free-Shop des Flughafens ist ein gutes Beispiel für einen derartigen Sensor, der entweder direkt durch den Shop, oder einen Zahlungsdienstleister dem der Shop vertraut, betrieben wird. Schwieriger wird es, wenn es um das Vertrauen zwischen dem Identity Agent und dem Sensor geht. Im Fall der Bezahlung in einem Shop soll Annas digitaler Zwilling nur dann die Rechnung bezahlen, wenn Anna das auch möchte. Die Bestätigung, dass Anna das möchte, kommt jedoch von einem Sensor, der von eben dem Shop betrieben wird, der durch die Zahlung profitieren würde.

Es gibt in der Praxis auch bereits Ansätze, welche diese Möglichkeit nutzen, um Benutzer*innen zu identifizieren. Ein Beispiel dafür sind die DTC-VC der ICAO (Rajeshkumar 2021), welche ein Reisedokument-Credential mit identifizierenden Attributen und biometrischen Merkmalen enthalten und dieses, als Gesamtpaket, der Einheit aus Sensor und Verifier (bzw. eigentlich einem Diensteanbieter, der sogar mehrere dieser Einheiten mit dem Credential versorgen kann) übergeben. Als Schutzmaßnahme, zur Abfederung der negativen Konsequenzen auf die Privatsphäre des betroffenen Individuums, ist die explizite, bewusste Weitergabe des Credentials durch dessen Inhaber*in vorgesehen (vgl. dazu auch Ahn und Lam 2005). So kann das ausgestellte Credential z. B. bei der Voranmeldung einer Auslandsreise an das Zielland übermittelt werden, um eine automatisierte Authentifizierung der Person beim späteren Grenzübertritt zu ermöglichen (Rajeshkumar 2021).

Eine Möglichkeit, um dieses Problem zu lösen, wären biometrische Zero-Knowledge-Proof (ZKP) Verfahren (vgl. Tran et al. 2022; Sakashita et al. 2009), die es dem Sensor ermöglichen würden, zu beweisen, dass er gerade die Biometrie einer bestimmten Person gemessen hat, ohne die Messdaten an den Identity Agent weiterzugeben. Allerdings sind diese ZKP-Verfahren nur für den $1:1$-Vergleich, also die biometrische Authentifizierung einer Person und nicht für den $1:N$-Abgleich, also die biometrische Identifizierung geeignet.

Weitere Ansätze sind Cancelable Biometrics (Manisha und Kumar 2020) und Verfahren auf Basis von homomorpher Kryptographie (Yang et al. 2020), die zwar für die biometrische Identifikation geeignet wären, aber aktuell noch zu langsam und ineffizient sind um die Echtzeitanforderungen vieler typischer Dienste (Zutrittskontrolle, Bezahlsysteme, etc.) zu erfüllen.

Zusammenfassend kann gesagt werden, dass die Dezentralisierung von Sensoren relativ einfach umsetzbar ist. Erst in Kombination mit der Dezentralisierung

der Identity Agents treten bisher ungelöste Probleme auf, weil es noch keine guten Technologien gibt, mit denen zwei Geräte sich gegenseitig beweisen können, dass sie über ein ausreichend ähnliches (aber nicht notwendigerweise bitgleiches) biometrisches Template verfügen, ohne die biometrischen Daten selbst zu enthüllen.

Ein Ansatz um dennoch Vertrauen in Sensoren aufzubauen, egal, wer die organisatorische Kontrolle darüber hat, könnte die unabhängige Verifizierbarkeit des Sensors, durch Attestierung eines nachweisbaren Hardware- und Softwarezustandes, der auch von unabhängigen Parteien prüfbar ist, bieten. Ein Hardware-Root-of-Trust könnte die Vertrauensbasis dazu liefern und die negativen Konsequenzen der organisatorischen Zugehörigkeit eines Sensors zum Dienst durch einen zusätzlichen Vertrauensanker abfedern. Damit hat der Identity Agent eine Möglichkeit zu prüfen, ob ein Sensor ausreichend sorgsam mit biometrischen Templates umgeht und diese nicht anderweitig nutzt oder selbst Verhaltensprofile von Individuen auf Basis der Vorregistrierung von Templates (durch einen Identity Agent der eine potentielle Sensorinteraktion vorhersieht) erstellt.

3.3 Dezentralisierung der Herausgeber

Der Schritt hin zu Attribute-Based-Access-Control (ABAC, vgl. Hu et al. 2014), also der Autorisierung basierend auf Eigenschaften einer Identität (z. B. Nachweis über Besitz einer gültigen Bordkarte), statt der Identität selbst (eindeutige Identifikation), zur Stärkung der Privatsphäre bei der organisatorischen Dezentralisierung von Diensten, eröffnet auch umfangreichere Möglichkeiten für die Dezentralisierung von Attribut-Herausgebern.

Dies findet sich bereits in verschiedenen bestehenden eID-Wallet-Konzepten wieder. Die europäische digitale Identität (Europäische Kommission 2021) soll Attribute aus öffentlichen und privaten Quellen in einer digitalen Brieftasche ermöglichen. SSI-Projekte (z. B. Sovrin, Windley 2021) etablieren Verifiable Credentials, Verifiable Presentations und Decentralized Identifiers als mögliche Datenformate für solche (verknüpften) Attribute und den Austausch einer selektiven Zusammenfassung von authentifizierbaren Attributen (vgl. Sporny et al. 2022a, b). Identity Agents können damit dienstspezifische, attributbasierte digitale Identitäten aus der Fülle der Attribute in der ID-Wallet zusammenstellen, und diese anonymen Attributkombinationen für die Authentifizierung und Autorisierung bei Diensten verwenden.

Die organisatorische Dezentralisierung von Herausgebern wird bei diesen Konzepten durch die Sammlung von Attributen in einer ID-Wallet ermöglicht. Durch die Konzentration in der Wallet wird die Komplexität der Interaktionen zwischen Herausgebern und Diensten in einen zentralen Punkt pro Interaktion (bzw. digitaler Identität oder sogar pro Individuum) gebündelt und damit reduziert. Gleichzeitig stärkt die organisatorische und räumliche Loslösung des Herausgebers vom Datenspeicher der Identitätsattribute für eine Stärkung der Privatsphäre, weil der Herausgeber nicht mehr in jede einzelne Transaktion involviert ist (vgl. Khatchatourov et al. 2015).

3.4 Dezentralisierung der Identity Agents

Als nächsten Schritt auf dem Weg zu einem dezentralen, offenen, globalen ID-Ökosystem betrachten wir die Dezentralisierung der digitalen Identität selbst bzw. des Identity Agent, der diese verwaltet. In klassischen zentralisierten Systemen wie Aadhaar werden diese zentral von einer Organisation gespeichert und verwaltet.

Im Gegenzug dazu müsste ein dezentraler Ansatz die organisatorische Verantwortung für den Identity Agent, im Sinne eines nutzerzentrierten Ansatzes, zu ihren Besitzer*innen verschieben. Damit einher ginge auch eine räumliche Dezentralisierung, da Nutzer*innen ihre digitalen Identitäten wohl kaum alle am gleichen Ort und mit der gleichen Infrastruktur betreiben würden. In diesem Sinne sollte es Individuen erlaubt sein, ihren digitalen Zwilling entweder selbst zu hosten, auf dem eigenen Smartphone laufen zu lassen (vgl. Konzept des Personal Authentication Device, Jøsang und Pope 2005), oder einen professionellen Anbieter mit dem Betrieb zu beauftragen.

Ideal wäre eine Verteilung der Identity Agents auf viele unterschiedliche Betreiber. Dies bringt den Vorteil, dass ein Datendiebstahl oder ein Ausfall eines Betreibers immer nur einen (kleineren) Teil der Nutzer*innen trifft. Es würde auch die Überwachungsmöglichkeiten jedes einzelnen Betreibers einschränken, da diese nur mehr die Interaktionen ihrer eigenen Nutzer*innen sehen.

Allerdings müssen sich nun viele Komponenten (N Sensoren und M Identity Agents bzw. M Identity Agents und L Verifier) gegenseitig finden und miteinander kommunizieren. Dadurch entstehen wiederum Seitenkanäle auf der Netzwerkebene, die von einem entsprechend ausgestatteten Angreifer ausgenutzt werden könnten:

- Durch die Interaktion von Sensoren mit bestimmten Identity Agents bzw. Identity Agents mit bestimmten Sensoren würde sich anhand der Beobachtung der Metadaten auf Netzwerkebene (Verbindungsaufbau von Agent X zu Sensor Y oder umgekehrt) ableiten lassen, bei welchen Sensoren, und damit an welcher geographischen Position, der digitale Zwilling sein modelliertes Individuum vermutet.
- Durch die, bei der Interaktion von Identity Agents mit bestimmten Verifiern anfallenden Metadaten würde sich analog dazu ableiten lassen, mit welchen Verifiern (und damit mit welchen Diensten) ein Individuum zu einem bestimmten Zeitpunkt interagiert.

Nach Hansen (2013) ist aber gerade in einem nutzerzentrischen ID-System Privatsphäre (im Sinne von Unlinkability) auch auf allen Netzwerkebenen entscheidend. Konzepte zum Einsatz von Netzwerkanonymisierungstechnologien wie Tor für die Interaktion in digitalen ID-Systemen (Höller et al. 2022) könnten hier Abhilfe schaffen.

Die Verteilung der Identity Agents in unterschiedlicher Infrastruktur wirft auch die Frage nach Mindestanforderungen in Hinblick auf Zuverlässigkeit und Reaktionszeit auf. Die Ausfallsicherheit und die Netzwerkanbindung eines Datencenters und eines einzelnen Smartphones sind nicht vergleichbar. Netzwerkanonymisierungstechnologien könnten hier einen zusätzlichen (zeitweisen) Engpass verursachen (vgl. aktuelle Überlastung des Tor-Netzwerks durch Denial-of-Service-Angriffe (Koppen 2022) oder Tor-Sperren in China (Tor Project 2022)).

Ähnlich dazu kann ein Identity Agent auf einem Smartphone nicht mit den Möglichkeiten eines hochperformanten Computerclusters mithalten. Dies geht einher mit der Frage, ob ein persönlicher Identity Agent sein Individuum ausreichend genau modellieren kann. Einerseits kann diese Genauigkeit durch die verfügbare Rechenleistung stark eingeschränkt sein (insb. wenn man dem Individuum bei der Wahl des Hostings viele Freiheiten lassen möchte). Andererseits stellt sich generell die Frage, ob ein einzelner Identity Agent überhaupt hinreichend genaue Vorhersagen treffen kann. Bestehende Ansätze legen hier eine bessere Modellierbarkeit vom Verhalten ganzer Gruppen (z. B. Vorhersage von Besucherströmen) oder von Rückschlüssen auf einzelne Individuen durch gemeinsame Modellierung des Verhaltens vieler Individuen nahe. Diese Fragen sind derzeit noch ungelöst und würden von einer Umsetzung erster Konzeptstudien profitieren.

Neben möglichen Seitenkanälen, Zuverlässigkeit und Reaktionszeit bei der Kommunikation stellt auch das gegenseitige Auffinden der Komponenten selbst ein komplexes Problem dar. In der bisherigen Betrachtung brachte die zentrale Identitätsdatenbank den Vorteil einer zentralen Anlaufstelle zwischen den N Sensoren, der globalen digitalen Identität und den L Verifiern. Die explizite Interaktion mit einem Sensor, der räumlich eindeutig einem Dienst zugeordnet ist, ergibt zudem eine 1 : 1-Beziehung aus Interaktion und Dienst.

Für Sensoren wäre es enorm schwierig, auf Basis von biometrischen Messwerten einen bestimmten Identity Agent zu finden, ohne dass biometrische Referenzdaten in einer öffentlichen Datenbank hinterlegt sind. Wenn Dienste organisatorisch von der Sensorik losgelöst sind, dann hat auch der Verifier keinerlei Anhaltspunkte dafür, dass ein Individuum mit einem Dienst interagieren möchte. Der Identity Agent kann hingegen aus dem Verhaltensmodell den Bewegungsradius des Individuums und damit für eine Interaktion in Frage kommenden Sensoren und Verifier gut einschränken, sofern ein (globaler) Überblick über mögliche Sensoren und Verifier vorhanden ist.

Um den Vorteil einer räumlich zentralen Anlaufstelle bei gleichzeitiger organisatorischer Dezentralisierung von Sensoren, Identity Agents und Diensten zu erzielen, könnten öffentliche Verzeichnisdienste zum Einsatz kommen. Nachdem Sensoren selbst, als öffentliches Objekt, keinen Privatsphäreschutz benötigen, könnten diese durch eine Datenbank, welche Sensoren einer geographischen Lage zuordnen, für alle Identity Agents auffindbar gemacht werden. Identity Agents können sich dann bei Sensoren vorregistrieren und, bei Übereinstimmung der Biometrie, über das Ereignis per Call-Back-Aufruf informiert werden. Ähnlich verhält es sich bei den Verifiern: Identity Agents können anhand der Sensorereignisse und des modellierten Verhaltens (eindeutig) bestimmen, mit welchem Verifier interagiert werden soll. Dabei kann auf Attribute als Informationen über bestehende (Geschäfts-)beziehungen des Individuums zu bestimmten Diensten, aber auch auf die Verknüpfung bestimmter Sensoren mit Diensten zurückgegriffen werden. Auch hierfür würde sich eine Datenbank, mit Informationen über das Vertrauen von Diensten in bestimmte Sensoren sowie mit Informationen über den (bzw. die) Verifier eines Dienstes, eignen.

Methoden zur Implementierung solcher Verzeichnisse könnten öffentliche Ledger (mit gleichzeitiger organisatorischer und räumlicher Dezentralisierung) oder klassi-

sche Verzeichnisdienste sein. Um die organisatorische Freiheit von Diensten und Sensoren nicht einzuschränken müssten diese Verzeichnisdienste jedoch für alle frei zugänglich gestaltet sein (d. h. auch ohne Einschränkungen bei der Eintragung neuer Sensoren und Dienste).

3.5 Dezentralisierung der ID-Wallet

Durch die enge Bindung von Identity Agent und ID-Wallet, als zugehöriger Datenspeicher, wird davon ausgegangen, dass eine organisatorische oder räumliche Trennung dieser beiden Rollen im Allgemeinen nicht zweckmäßig ist. Es gibt jedoch auch Ausnahmen:

- Biometrische Sensoren können fest an ein einzelnes Individuum geknüpft sein (z. B. in einem mitgeführten Smartphone). Wenn der Sensor ausschließlich für den Identity Agent vertrauenswürdig sein muss, dann macht es Sinn, die biometrischen Referenzdaten ausschließlich in diesem Sensor abzulegen, um Missbrauchspotential zu minimieren. Dies ist der Fall, wenn vom Sensor nur Verhalten abgeleitet wird (und das Individuum ein Interesse am akkuraten Verhalten des Sensors hat) oder wenn für den Verifier die Bindung zwischen biometrischem Merkmal und der Identität nicht relevant ist, weil die Verantwortung an das Individuum abgegeben werden kann (z. B. Freigabe einer Transaktion durch Fingerabdruck am eigenen Smartphone).
- Attribute, die ausschließlich für einen einzelnen Dienst oder sogar einen Aktor relevant sind (z. B. Zutrittsberechtigungen in einer Firma), können, statt in einer nutzerzentrischen ID-Wallet, auch beim Dienst selbst verwaltet werden, und nur über pseudonyme Authentifizierung an eine digitale Identität gebunden werden. Sie sind damit organisatorisch und räumlich von der restlichen ID-Wallet entkoppelt und obliegen der Verantwortung des Dienstes. Die Inhalte solcher Attribute können damit aber auch nicht für die Modellierung im Identity Agent herangezogen werden.

Abgesehen davon bringt, wie bereits für den Identity Agent selbst, die organisatorische und räumliche Dezentralisierung der ID-Wallet zusammen mit dem Identity Agent auf den ersten Blick gleich mehrere Vorteile für das Individuum: Die Verteilung der (biometrischen) Daten der Nutzer*innen auf viele verschiedene Orte und Betreiber eliminiert einen zentralen Single-Point-of-Failure. Ein Ausfall oder ein Datendiebstahl bei einem einzelnen Betreiber trifft damit nur mehr einen vergleichsweise kleinen Teil der Nutzer*innen. Nachdem keine zentrale Stelle alle biometrischen Daten besitzt und diese auch nicht bei der Verifikation durch Dienste zum Einsatz kommen, wird die Möglichkeit einer (flächendeckenden) biometrischen Überwachung oder Beschränkung durch Einzelne (z. B. einen Staat) minimiert.

Bei genauer Betrachtung entstehen dadurch aber auch neue Probleme: Gezielte Angriffe auf ein Individuum sind durch Angriffe auf einen einzelnen Identity Agent weiter möglich. Das Schadensausmaß bei einem Datendiebstahl ändert sich für das einzelne betroffene Individuum nicht. Die Verteilung auf mehrere Betreiber (und ggf. das Individuum selbst) reduziert sogar die (insb. finanziellen) Möglichkeiten

einzelner zur Absicherung ihrer Systeme, und könnte damit individuelle Angriffe noch attraktiver gestalten.

Zudem stellt ein attributzentriertes ID-System, bei dem Attribute aus einer dezentralen ID-Wallet zu beliebigen Zusammenstellungen (vgl. Verifiable Presentations) kombiniert werden sollen, hohe Ansprüche an die Sicherheit kryptographischer Komponenten. Selbst der uneingeschränkte Zugriff der Nutzer*in selbst auf eigene geheime kryptographische Schlüssel kann problematisch sein. Zwei kollaborierende Nutzer*innen dürfen z. B. aus der Kombination ihrer Attribute keinen Vorteil erlangen können. Lösungen könnten in der Auslagerung kritischer kryptographischer Komponenten in zertifizierte Hardware-Security-Module (HSMs) bzw. Smartcards/Secure Elements liegen. Dadurch können sicherheitskritische Teile der ID-Wallet räumlich zur Nutzer*in und gleichzeitig organisatorisch zu einem vertrauenswürdigen Dritten verlagert werden (ähnlich wie der Hardware-Root-of-Trust-Ansatz für Sensoren). Aktuell hinken Smartcard-Chips jedoch bei der Umsetzung moderner, privatsphäreschonender kryptographischer Verfahren (z. B. ZKP-Verfahren) hinterher.

Während SSI-Projekte die gesamte Wallet-Komponente organisatorisch und räumlich verteilen möchten und näher in Richtung der Nutzer*in bringen, finden sich in bestehenden nationalen eID-Wallet-Konzepten andere Strategien. Bei der ID-Austria (A-SIT Plus GmbH 2021b) wird lediglich die Berechtigungsverwaltung für den Zugriff auf Attribute den Nutzer*innen anvertraut. Der Datenspeicher selbst liegt aber organisatorisch und räumlich bei einem staatlichen Anbieter. Auch der Vorschlag der EU-Kommission für eine europäische digitale Identität (Europäische Kommission 2021) spricht nur von einer nutzerzentrischen Verwaltung der Identität durch appgestützte Wallets, nicht aber von Dezentralisierung der eigentlichen Datenhaltung. Das SDI-Schaufensterprojekt ONCE[8] verfolgt hingegen eine Mischform aus Verwaltung des Zugriffs auf hoheitliche ID-Schemata und vollständig dezentralen SSI-Credentials (ONCE 2022).

Abschließend bleibt die Frage, wie der Identity Agent entscheidet, welche Attribute aus der Wallet an einen Verifier weitergegeben werden dürfen. Bei organisatorischer Zentralisierung (insb. der Identity Agents) könnte diese Entscheidung vollständig durch den Betreiber des ID-Systems abgenommen werden (vgl. Registrierungserfordernis für Verifier). In einem nutzerzentrischen System, sollte dies vom Individuum entschieden (oder zumindest mitbestimmt) werden können, um organisatorische Freiheit der Dienste und der Identity Agents zu erzielen. Wenn jeder Identity Agent unabhängig ist und das System völlig offen für jeden Verifier sein soll, dann wird es für einzelne Nutzer*innen unverhältnismäßig und unüberschaubar, den Überblick über Sinn und Zweck angeforderter Attribute zu behalten. Hansen (2013) schlägt daher die Ausstellung von Zertifikaten über Attributprofile durch vertrauenswürdige Stellen vor. Eine Möglichkeit dies in einem offenen System umzusetzen, könnte wiederum in den Verzeichnisdiensten für Sensoren und Verifier liegen. Dort könnten Dienste Attributprofile veröffentlichen und von unabhängigen Drittstellen begutachten lassen. Solche Drittstellen könnten beispielsweise Bürger-

[8] https://once-identity.de/.

rechtsorganisationen sein, die das Verzeichnis um Zertifikate über die geprüften Profile ergänzen.

4 Dezentrales, offenes, globales Ökosystem zur privaten, digitalen Authentifizierung in der physischen Welt

Auf Basis dieser Abwägungen lässt sich ein erstes Konzept für ein dezentrales, offenes, globales Ökosystem zur privaten, digitalen Authentifizierung in der physischen Welt skizzieren. Abb. 2 gibt einen Überblick über diese Architektur, die wesentlichen Interaktionen bei ID-Transaktionen und die abgeleiteten Vertrauensbeziehungen (vgl. auch Mayrhofer et al. 2020):

- Das Individuum ist eine natürliche Person, die in der physischen Welt agiert. Als Nutzer*in des ID-Ökosystems ist das Individuum Inhaber*in einer (oder sogar mehrerer) digitaler Identitäten. Diese werden in Form von Sammlungen von authentifizierten Attributen durch verschiedene Herausgeber attestiert.
- Bei ihren Handlungen in der physische Welt interagiert die Nutzer*in laufend mit verschiedenen Sensoren. Dies können explizite Interaktionen (wie z. B. das Auflegen des Fingers auf ein Fingerabdrucklesegerät) oder implizite Interaktionen (wie z. B. das Vorbeigehen an einer Videokamera) sein.
- Der Personal Identity Agent (PIA) repräsentiert, als digitaler Zwilling, das Individuum in der digitalen Welt. Der PIA verwaltet, als ID-Wallet, die Sammlung an digitalen Identitäten des Individuums und modelliert dessen Verhalten um möglichst exakte Vorhersagen über Interaktionen in der physischen Welt zu treffen.
- Auf Basis dieser Vorhersagen nimmt der PIA Kontakt mit jenen vertrauenswürdigen Sensoren auf, die für anstehende Interaktionen in Frage kommen könnten und stellt diesen biometrische Referenzdaten zur Identifikation des Individuums in einem beschränkten Zeitfenster zur Verfügung. Mögliche Sensoren können anhand öffentlicher Listen und Anforderungen spezifischer Dienste gefunden werden. Im Idealfall wird dieser direkte Austausch biometrischer Merkmale in Zukunft durch neue Entwicklungen im Bereich der biometrischen ZKP-Verfahren oder der homomorphen Kryptographie ersetzbar. Auch in diesem Fall wird eine Voranmeldung potentieller Interaktionen bei Sensoren durch den PIA zur Skalierbarkeit der Service Discovery beitragen.
- Die Sensoren liefern daraufhin bei erfolgter Identifikation authentifizierte Belege über die Identifikation und gemessene Ereignisse (z. B. Individuum bewegt sich auf Tür bzw. Sensor zu) an den PIA. Dieser nutzt die gelieferten Ereignisse und verknüpft sie mit vorhanden Informationen der ID-Wallet um Bewegungsabläufe, Verhalten und Gewohnheiten des Individuums zu modellieren.
- Auf Basis erkannter Intentionen löst der PIA eine Authentisierung beim Verifier des zuständigen Dienstes aus und übermittelt eine Präsentation der notwendigen Identitätsattribute und ggf. Beweise für Sensorereignisse, welche die Berechtigung zur Nutzung des Dienstes belegen (vgl. Verifiable Presentation bei SSI). Die für einen Dienst unbedingt erforderlichen Attribute können transparent in öffentlichen

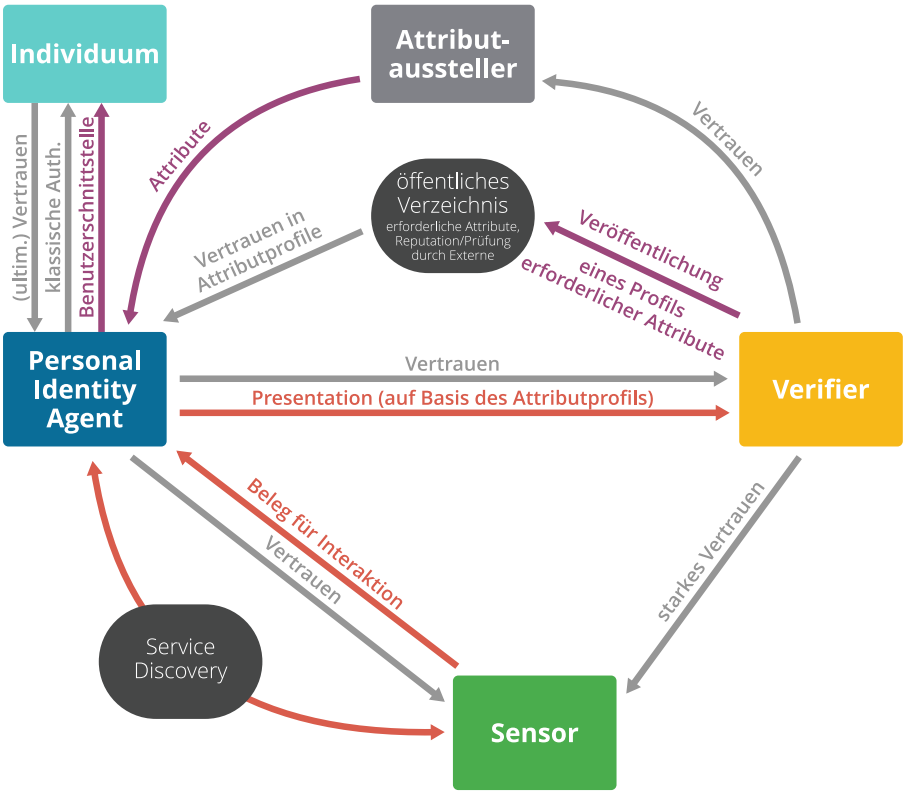

Abb. 2 Architekturkonzept für ein dezentrales, offenes, globales ID-Ökosystem

Listen für jeden einsehbar abgelegt werden, um das erforderliche Vertrauen des PIA für die Herausgabe von Attributen zu gewährleisten.

- Darüber hinaus bietet der PIA dem Individuum eine Benutzerschnittstelle (z. B. in Form einer Companion-App am Smartphone) über die ggf. explizite Freigaben für bestimmte Transaktionen erfolgen können.

5 Fazit und Ausblick

Kontinuierliche, implizite biometrische Identifikation zur Authentifizierung über die Grenzen der physischen und digitalen Welt hinweg ist von einer Zukunftsvision der Science Fiction längst zu einer greifbaren Möglichkeit geworden. Solche ID-Systeme sind bereits jetzt relativ einfach durch zentrale biometrische Datenbanken, mit umfangreichen Überwachungsmöglichkeiten, umsetzbar. Derzeit in Europa auf breite Ablehnung und Unvereinbarkeit mit geltendem Recht stoßend, könnten Vorteile aus der Technologie – nicht zum ersten Mal – rasch zu einem Umdenken und einer Umgestaltung der rechtlichen Rahmenbedingungen führen. Um für einen solchen Fall auch technologisch gerüstet zu sein, ist es essentiell, den Schutz der

Privatsphäre jedes einzelnen Individuums bereits bei der Konzeptionierung solcher ID-Systeme als fixen Bestandteil einzuplanen. Wir evaluieren, welcher Zugewinn an Privatsphäreschutz durch die organisatorische und räumliche Dezentralisierung der Komponenten des ID-Systems und eine Öffnung und Nutzerzentrierung der digitalen Identität liefern kann und welche (neuen) Probleme damit einhergehen, die diesen Privatsphäreschutz impraktikabel machen. Aus den Erkenntnissen heraus entwickeln wir ein Konzept für ein dezentrales, offenes, globales Ökosystem zur privaten, digitalen Authentifizierung in der physischen Welt auf Basis digitaler Zwillinge, das die Ausgangsbasis für weitere Studien bilden soll.

Die Analyse des State-of-the-Art zeigt, das insbesondere die Dezentralisierung von Diensten und Attribut-Herausgebern bereits weitgehend umsetzbar ist und Entwicklungen im Bereich der pseudonymen und anonymen Authentifizierung guten Privatsphäreschutz ermöglichen. Während bei Sensoren die räumliche Dezentralisierung ein gelöstes Problem darstellt, führt organisatorische Unabhängigkeit unweigerlich zur Verarbeitung biometrischer Daten jedes Individuums über viele Vertrauensdomänen hinweg. Die wesentlichste, noch nicht ausreichend gelöste technologische Hürde stellt der Abgleich biometrischer Daten in einer großen (globalen) Population ohne tatsächlichen Austausch von biometrischen Merkmalen dar. Übergangsstrategien versuchen die Verantwortung der Sensoren für biometrische Daten auf kleine Subsets der Teilnehmer am ID-System einzugrenzen und Sensoren mit unabhängigen, verifizierbaren Vertrauensankern auszustatten.

Die organisatorische und räumliche Verlagerung des Identity Agents zur Nutzer*in stellt jedoch das größte ungelöste Problem dar. Zwar wirkt sich eine Teilung der Verantwortung über die Daten im ID-System grundsätzlich vorteilhaft auf die Sicherheit und Privatsphäre jedes einzelnen aus, gleichzeitig gehen damit aber neue Risiken einher, die bisher nur unzureichend betrachtet wurden. Beispiele dafür sind Privatsphäre gefährdende Seitenkanäle aufgrund zusätzlicher Netzwerkkommunikation, fehlende Ansätze zur individuellen Modellierung persönlicher Verhaltensprofile, fehlende Daten zur Zuverlässigkeit und Reaktionszeit (sowohl in Hinblick auf die Netzwerkkommunikation, die Modellierung des digitalen Zwillings, die Service Discovery, als auch auf die breiten Streuungsmöglichkeiten beim Selbsthosting eines PIA). Diese offenen Fragen sollen anhand der Weiterentwicklung des präsentierten Konzepts studiert werden.

Danksagung Diese Arbeit entstand im Rahmen von ONCE (FFG-Projektnummer FO999887054), gefördert im Programm „IKT der Zukunft“ vom Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK), und Digidow, dem Christian-Doppler-Labor für Private Digitale Authentifizierung in der physischen Welt, gefördert vom Bundesministerium für Arbeit und Wirtschaft (BMAW) und der Nationalstiftung für Forschung, Technologie und Entwicklung, und unterstützt von 3 Banken IT GmbH, ekey biometric systems GmbH, Kepler Universitätsklinikum GmbH, NXP Semiconductors Austria GmbH & Co KG, und Österreichische Staatsdruckerei GmbH.

Funding Open access funding provided by Johannes Kepler University Linz.

Literatur

Ahn GJ, Lam J (2005) Managing Privacy Preferences for Federated Identity Management. In: DIM '05: Proceedings of the 2005 Workshop on Digital Identity Management, ACM, S 28–36 https://doi.org/10.1145/1102486.1102492

Ates M, Ravet S, Ahmat AM, Fayolle J (2011) An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and Other Delights. In: 2011 Sixth International Conference on Availability, Reliability and Security, IEEE, S 555–560 https://doi.org/10.1109/ARES.2011.85

Austrian Federal Chancellery, Federal Platform Digital Austria (Hrsg) (2014) Administration on the Net: The ABC guide of eGovernment in Austria. Kny & Partner, Vienna

A-SIT Plus GmbH (2021a) ID Austria: Technisches Whitepaper für Service-Owner. https://eid.egiz.gv.at/wp-content/uploads/2021/10/ID-Austria-Technisches-Whitepaper-fuer-Service-Owner-1.pdf. Zugegriffen: 21. Dezember 2022

A-SIT Plus GmbH (2021b) ID Austria: Technisches Whitepaper für Endnutzer*innen. https://eid.egiz.gv.at/wp-content/uploads/2021/12/ID-Austria-Whitepaper-fuer-EndanwenderInnen.docx.pdf. Zugegriffen: 21. Dezember 2022

Barricelli BR, Casiraghi E, Fogli D (2019) A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications. IEEE Access 7:167653–167671. https://doi.org/10.1109/ACCESS.2019.2953499

BGBl I Nr 190/1999 (1999) Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG). BGBl. für die Republik Österreich, Teil I, Nr. 190/1999, S 1451–1462

Bonnette R (2017) Biometrics in Movies Sci-Fi Security. The Identity & Access Management Blog. https://www.avatier.com/blog/biometrics-in-sci-fi-movies/. Zugegriffen: 14. September 2022

Bundesministerium für Finanzen (2022) Informationen zu Stufen der ID Austria und zur Pilotphase. https://www.oesterreich.gv.at/id-austria/pilotbetrieb.html#digitale-ausweise. Zugegriffen: 14. September 2022

Camenisch J, Dubovitskaya M, Enderlein RR, Lehmann A, Neven G, Paquin C, Preiss FS (2014) Concepts and languages for privacy-preserving attribute-based authentication. J Inf Secur Appl 19(1):25–44. https://doi.org/10.1016/j.jisa.2014.03.004

Chivers H (2005) Personal Attributes and Privacy: How to ensure that private attribute management is not subverted by datamining. In: Chadwick D, Preneel B (Hrsg) Communications and multimedia security. IFIP advances in information and communication technology (IFIPAICT), Bd. 175. Springer, Boston, MA, S 17–29 https://doi.org/10.1007/0-387-24486-7_2

Danezis G, Domingo-Ferrer J, Hansen M, Hoepman JH, Le Métayer D, Tirtea R, Schiffner S (2014) Privacy and Data Protection by Design – from policy to engineering. European Union Agency for Network and Information Security (ENISA) https://doi.org/10.2824/38623

Europäische Kommission (2021) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität. COM(2021) 218 final. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0281. Zugegriffen: 14. September 2022

Grieves M, Vickers J (2017) Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In: Kahlen FJ, Flumerfelt S, Alves A (Hrsg) Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches. Springer, Cham, S 85–113 https://doi.org/10.1007/978-3-319-38756-7_4

Hansen M (2013) Data Protection by Default in Identity-Related Applications. In: Fischer-Hübner S, de Leeuw E, Mitchell C (Hrsg) Policies and research in identity management. IFIP advances in information and communication technology (IFIPAICT), Bd. 396. Springer, Berlin, Heidelberg, S 4–17 https://doi.org/10.1007/978-3-642-37282-7_2

Höller T, Roland M, Mayrhofer R (2022) Evaluating Dynamic Tor Onion Services for Privacy Preserving Distributed Digital Identity Systems. J Cyber Secur Mobil 11(2):141–164. https://doi.org/10.13052/jcsm2245-1439.1122

Hölzl M, Roland M, Mir O, Mayrhofer R (2018) Bridging the Gap in Privacy-Preserving Revocation: Practical and Scalable Revocation of Mobile eIDs. In: Proceedings of the ACM SAC Conference (SAC '18), ACM, S 1601–1609 https://doi.org/10.1145/3167132.3167303

Hu V, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. https://doi.org/10.6028/NIST.SP.800-162

ICAO Doc 9303 (2021) Machine Readable Travel Documents, Part 1 — Introduction, 8. Aufl.

ISO/IEC 18013-2:2020 (2020) Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies

ISO/IEC 18013-5:2021 (2021) Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

ISO/IEC FDIS 23220-1 (2022) Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems

Jøsang A, Pope S (2005) User Centric Identity Management. In: Proceedings of AusCERT Conference 2005. https://folk.uio.no/josang/papers/JP2005-AusCERT.pdf. Zugegriffen: 14. September 2022

Khaira R (2018) Rs 500, 10 minutes, and you have access to billion Aadhaar details. The Tribune. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361. Zugegriffen: 14. September 2022

Khatchatourov A, Laurent M, Levallois-Barth C (2015) Privacy in Digital Identity Systems: Models, Assessment, and User Adoption. In: Tambouris E, Janssen M, Scholl HJ, Wimmer MA, Tarabanis K, Gascó M, Klievink B, Lindgren I, Parycek P (Hrsg) Electronic government. Lecture notes in computer science (LNCS), Bd. 9248. Springer, Cham, S 273–290 https://doi.org/10.1007/978-3-319-22479-4_21

Koning M, Korenhof P, Alpár G, Jaap-Henk H (2014) The ABCs of ABCs – An Analysis of Attribute-Based Credentials in the Light of Data Protection, Privacy and Identity. In: 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2014). https://www.petsymposium.org/2014/papers/Koning.pdf. Zugegriffen: 14. September 2022

Koppen G (2022) DoS attacks – status update. Message on tor-relays mailing list. https://lists.torproject.org/pipermail/tor-relays/2022-October/020858.html. Zugegriffen: 21. Dezember 2022

Manisha, Kumar N (2020) Cancelable Biometrics: a comprehensive survey. Artif Intell Rev 53:3403–3446. https://doi.org/10.1007/s10462-019-09767-8

Mayrhofer R, Roland M, Höller T (2020) Poster: Towards an Architecture for Private Digital Authentication in the Physical World. In: Network and Distributed System Security Symposium (NDSS Symposium 2020), Posters

ONCE (2022) Das Projekt: Hoheitliche Daten und Self Sovereign Identity. Once – Identity. https://once-identity.de/das-projekt/. Zugegriffen: 21. Dezember 2022

Phillips DJ (2004) Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. New Media Soc 6(6):691–706. https://doi.org/10.1177/146144804042523

Poller A, Waldmann U, Vowe S, Turpe S (2012) Electronic Identity Cards for User Authentication—Promise and Practice. IEEE Secur Privacy 10(1):46–54. https://doi.org/10.1109/MSP.2011.148

Qian I, Xiao M, Mozur P, Cardia A (2022) Four takeaways from a times investigation into China's expanding surveillance state. The New York Times. https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html. Zugegriffen: 21. Dezember 2022

Rajeshkumar R (2021) Digital travel credentials. https://www.icao.int/Meetings/TRIP-Symposium-2021/PublishingImages/Pages/Presentations/Digital%20Travel%20Credential%20%28DTC%29%20Policy%20and%20Guiding%20Principles.pdf. Zugegriffen: 14. September 2022

Richtlinie 1999/93/EG (2000) Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. Amtsblatt der Europäischen Gemeinschaften, Nr. L 13 vom 19.01.2000, S. 12–20. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:31999L0093. Zugegriffen: 14. September 2022

Sakashita T, Shibata Y, Yamamoto T, Takahashi K, Ogata W, Kikuchi H, Nishigaki M (2009) A Proposal of Efficient Remote Biometric Authentication Protocol. In: Takagi T, Mambo M (Hrsg) Advances in information and computer security. Lecture notes in computer science (LNCS), Bd. 5824. Springer, Berlin, Heidelberg, S 212–227 https://doi.org/10.1007/978-3-642-04846-3_14

Schaber F, Strauß S, Peissl W (2020) Der Körper als Schlüssel? Biometrische Methoden für Konsument*innen. https://www.arbeiterkammer.at/service/studien/konsument/Der_Koerper_als_Schluessel.html. Zugegriffen: 14. September 2022

Schlager C, Nowey T, Montenegro JA (2006) A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce. In: First International Conference on Availability, Reliability and Security (ARES'06), IEEE. https://doi.org/10.1109/ARES.2006.13

Sporny M, Longley D, Chadwick D (2022a) Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model. Zugegriffen: 21. Dezember 2022

Sporny M, Longley D, Sabadello M, Reed D, Steele O, Allen C (2022b) Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core. Zugegriffen: 21. Dezember 2022

Tor Project (2022) How to circumvent the Great Firewall and connect to Tor from China? Tor project support. https://support.torproject.org/censorship/connecting-from-china/. Zugegriffen: 21. Dezember 2022

Tran QN, Turnbull BP, Wang M, Hu J (2022) A Privacy-Preserving Biometric Authentication System with Binary Classification in a Zero Knowledge Proof Protocol. IEEE Open J Comput Soc 3(1):1–10. https://doi.org/10.1109/OJCS.2021.3138332

Unique Identification Authority of India (2022) Authentication Ecosystem: Operational Model. https://www.uidai.gov.in/en/ecosystem/authentication-ecosystem/operation-model.html. Zugegriffen: 14. September 2022

Verordnung (EU) 2016/679 (2016) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Amtsblatt der Europäischen Union, Nr. L 119 vom 04.05.2016, S. 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj

Verordnung (EU) Nr. 910/2014 (2014) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Amtsblatt der Europäischen Union, Nr. L 257 vom 28.08.2014, S. 73–114, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:32014R0910

Windley PJ (2021) Sovrin: An Identity Metasystem for Self-Sovereign Identity. Front Blockchain. https://doi.org/10.3389/fbloc.2021.626726

Yang W, Wang S, Yu K, Kang JJ, Johnstone MN (2020) Secure Fingerprint Authentication with Homomorphic Encryption. In: 2020 Digital Image Computing: Techniques and Applications (DICTA), IEEE, S 1–6 https://doi.org/10.1109/DICTA51227.2020.9363426

Zwingelberg H, Hansen M (2011) Privacy Protection Goals and Their Implications for eID Systems. In: Camenisch J, Crispo B, Fischer-Hübner S, Leenes R, Russello G (Hrsg) Privacy and identity management for life. IFIP advances in information and communication technology (IFIPAICT), Bd. 375. Springer, Berlin, Heidelberg, S 245–260 https://doi.org/10.1007/978-3-642-31668-5_19